CLAIMS

1. Electrical device (14) for connection to a predetermined network (10) containing at least one watchdog device (12), where said electrical device comprises:

- storage means (20),
- configuration means (26) for authorising its operation in the presence of said watchdog device (12),
- means (28) for identifying at least one watchdog device when the electrical device is connected to any network containing such a watchdog device; and
- means (30) for disabling the electrical device (14) if the watchdog device identified does not correspond to the watchdog device (12) for which it was configured or if said network does not contain a watchdog device, characterised in that the configuration means (26) are suitable for recording a public identifier (V) of the watchdog device (12) for which the electrical device is configured, in the storage means (20).

2. Electrical device (14) according to claim 1, characterised in that the identification means (28) comprise means for interrogating any watchdog device to determine its public identifier (V).

3. Electrical device (14) according to any one of claims 1 or 2, characterised in that the identification means (28) comprise means for authenticating the watchdog device (12) for which it was configured.

4. Electrical device (14) according to claim 3, characterised in that the authentication means implement a zero-knowledge challenge/response protocol.

5. Electrical device (14) according to any one of claims 1 or 2, characterized in that it is in a state chosen from one of the elements of the assembly comprising a virgin state (32), a configured state (34) for operating in the presence of at least one watchdog device (14) and a blocked state (36), the configured state (34) being obtained after activation of the configuration means

(26) and the blocked state (36) being obtained after activation of the disabling means (30).

6. Electrical device (14) according to claim 5, characterized in that it operates only when it is in the configured state (34).

7. Antitheft system comprising at least one network (10) and at least one watchdog device (12) connected to the network and containing a public identifier (V), characterized in that it includes at least one electrical device (14) according to any one of claims 1 to 6.

8. Anti-theft system according to claim 7, characterized in that the watchdog device (12) comprises secure means (16) for storing a secret identifier (S) from which the public identifier (V) is generated.

9. Antitheft system according to claim 8 or 9, characterized in that the network (10) is chosen from among one of the elements of the group comprising an electric network, a digital transmission network and a telecommunications network.

10. Method for pairing a first (12) and second (14) device, where the second device (14) is designed to be connected to a network (10) that is connected to the first "watchdog" device (12), said method comprising a step of configuration (38) of the second device (14) to authorize its operation only in the presence of the watchdog device (12), characterized in that the step of configuration (38) of the second device (14) comprises the recording, in storage means (20) of the second device (14), of a public identifier (V) of the watchdog device (12).

11. Pairing method according to claim 10, characterized in that the second device (14) is in a state selected from among one of the elements of the assembly made up of a virgin state (32), of a state (34) configured to operate in the presence of at least one watchdog device (12) and a blocked state (36), and in that the configuration step (38) contains a change in state of the second device (14), from the virgin (32) to the configured state (34).

12 Pairing method according to claim 11, characterized in that it comprises a step of disabling (40) the second device (14) when this device is connected to a watchdog device for which it was not configured, where this disabling step comprises a change of state of the second device (14), from the configured state (34) to the blocked state (36).

13. Pairing method according to claim 11 or 12, characterized in that it comprises a step of identifying a watchdog device connected to a network, when the second device (14) is connected to this network.

14. Pairing method according to claim 13, characterized in that the identification step is triggered by one of the triggering events from the set of events constituted by a connection of the second device (14) to the network, a start up of the second device and a regular or random identification program.

15. Pairing method according to claim 13 or 14, characterized in that the identification step comprises the authentication of the watchdog device.

16. Pairing method according to claim 15, characterized in that the authentication step is realised by the use of a zero-knowledge challenge/response protocol.

17. Pairing method according to claim 16, characterized in that, the watchdog device (12) comprising means (16) for secure storage of a secret identifier (S) from which a public identifier (V) is generated, the identification comprises a step of interrogating the watchdog device to determine its public identifier (V) and the authentication comprises a series of steps during which the watchdog device (12) proves to the electrical device (14) that it knows the secret identifier (S) using the zero-knowledge challenge/response protocol.

18. Pairing method according to any one of claims 13 to 17, characterized in that if the identification step concludes that the network contains the watchdog device (12) for which the second device (14) was configured whereas the second device is in the blocked state, it is followed by a change in state of the second device (14) from the blocked state (36) to the configured state (34).